

ESTRUCTURAS ORDENADAS

Ordenes y Retículos *

Renato Lewin
Pontificia Universidad Católica de Chile

Julio de 1998

1 Conjuntos Ordenados

1.1 Definición y Ejemplos

Un *conjunto parcialmente ordenado*, o simplemente un *orden parcial*, es un par $\langle P, \leq \rangle$ donde P es un conjunto no vacío y \leq es una relación binaria sobre P que verifica:

O1 (Reflexividad)

Para todo $x \in P$, $x \leq x$.

O2 (Antisimetría)

Si $x \leq y$ y $y \leq x$, entonces $x = y$.

O3 (Transitividad)

Si $x \leq y$ y $y \leq z$, entonces $x \leq z$.

Si además \leq verifica:

*Estas notas han sido preparadas para un Cursillo dictado en la Primera Escuela de Postgrado de Invierno, organizada por la Facultad de Matemática de la Pontificia Universidad Católica de Chile en julio de 1998.

O4 (Conexión)

Para todo $x, y \in P$, $x \leq y$ ó $y \leq x$.

decimos que el orden es *total* o *lineal* o que P es *totalmente ordenado*.

Si no existe el peligro de confusión, hablaremos del conjunto ordenado P en lugar de $\langle P, \leq \rangle$ y usaremos el mismo símbolo, \leq para la mayoría de nuestros órdenes. Escribiremos $a < b$ para abreviar $a \leq b$ y $a \neq b$. También $b \geq a$ será sinónimo de $a \leq b$.

EJEMPLOS

1. Los conjuntos de números \mathbb{N} , \mathbb{Z} , \mathbb{Q} y \mathbb{R} con su orden habitual, es decir, magnitud, son conjuntos totalmente ordenados.
2. $\langle \mathbb{N}, | \rangle$ donde la relación de orden esta dada por

$$x|y \text{ si y sólo si } x \text{ divide a } y,$$

es un orden.

3. El conjunto de los divisores de un entero positivo n , ordenados como en el ejemplo anterior por la relación de divisibilidad, es también un orden.
4. Si X es un conjunto y $P \subseteq \mathcal{P}(X)$, donde $\mathcal{P}(X)$ es el conjunto de todos los subconjuntos de X , entonces $\langle P, \subseteq \rangle$ es un orden. Llamaremos a estos *órdenes de conjuntos*.
5. Sobre $\mathbb{Z} \times \mathbb{Z}$, el conjunto de los pares ordenados de números enteros, se define el *orden producto*

$$(a, b) \leq (c, d) \text{ si y sólo si } a \leq c \text{ y } b \leq d.$$

6. El ejemplo anterior se puede generalizar a cualquier número de ordenes. Si para cada $i = 1, 2, \dots, n$, $\langle P_i, \leq_i \rangle$ es un orden, entonces $\langle P_1 \times P_2 \times \dots \times P_n, \leq \rangle$, donde

$$(a_1, \dots, a_n) \leq (b_1, \dots, b_n) \text{ si y sólo si } a_i \leq_i b_i \text{ para todo } i = 1, \dots, n,$$

es un orden.

7. El orden anterior es bastante natural para el conjunto $\mathbb{Z} \times \mathbb{Z}$. Sin embargo existen otras maneras de ordenarlo y que también resultan “naturales”. Definamos

$$(a, b) \leq (c, d) \text{ si y sólo si } a < c \text{ o bien } a = c \text{ y } b \leq d.$$

Denotamos este orden $\langle \mathbb{Z} \otimes \mathbb{Z}, \leq \rangle$ y lo llamamos el orden *lexicográfico* sobre $\mathbb{Z} \times \mathbb{Z}$.

8. Es claro que el orden lexicográfico puede también extenderse a productos cartesianos de cualquier número de ordenes totales.
9. El conjunto ${}^{\mathbb{R}}\mathbb{R}$ de todas las funciones $f : \mathbb{R} \longrightarrow \mathbb{R}$ se puede ordenar como sigue:

$$f \leq g \text{ si y sólo si } f(x) \leq g(x) \text{ para todo } x \in \mathbb{R}.$$

Este es en realidad una generalización del orden producto.

10. Más generalmente, dado un orden $\langle P, \leq \rangle$ y un conjunto cualquiera I (no necesariamente ordenado), el conjunto ${}^I P = \{f : I \longrightarrow P\}$ ordenado como en el ejemplo anterior es también un orden.
11. Si $\langle P, \leq \rangle$ es un orden, entonces $\langle P, \leq^* \rangle$, donde

$$x \leq^* y \text{ si y sólo si } y \leq x,$$

es también un orden, llamado el orden inverso de \leq , habitualmente denotado P^* .

12. Dado un orden $\langle P, \leq \rangle$, cualquier subconjunto $Q \subseteq P$ ordenado por la restricción del orden de P a Q es también un orden, llamado el *orden heredado*. Decimos que Q es un *suborden* de P .

Un elemento del orden P se dice *minimal* si no existe ningún elemento que sea menor que él. Similarmente, un elemento es *maximal* si no hay elementos mayores que él.

Es importante no confundir elementos minimales (maximales) con el mínimo (máximo) elemento de P .

Ejemplos

1. Consideramos el orden $\langle \mathcal{P}(X) - \{\emptyset\}, \subseteq \rangle$. Este orden no tiene mínimo, sin embargo todo singleton $\{x\}$, con $x \in X$, es un elemento minimal. Obviamente X es el máximo.
2. Si X es un conjunto infinito y $\mathcal{P}_0(X)$ es el conjunto de los subconjuntos finitos de X , entonces $\langle \mathcal{P}_0(X), \subseteq \rangle$ no tiene elementos maximales. En este caso \emptyset es el único elemento minimal y por ende es el menor elemento.

Diremos que b cubre a a , en símbolos $a \prec b$, si $a < b$ y no existe otro elemento entre ellos, i.e. no existe $c \neq a, b$, tal que $a < c < b$.

Una *cadena* dentro del orden P es un subconjunto totalmente ordenado.

1.2 Diagramas de Hasse

Es habitual representar gráficamente ciertos órdenes usando los llamados diagramas de Hasse. Para ello, cada elemento o “punto” del orden se representa por un pequeño círculo \circ de tal manera que si $a < b$, el círculo que representa a a se ubica más abajo que aquel que representa a b y cuando b cubre a a , se unen ambos círculos con una recta. En el caso de órdenes finitos no muy complejos, se puede hacer un diagrama completo, pero el método es ilustrativo incluso para órdenes infinitos. Ver la Figura 1.

1.3 Isomorfismos

Una función $\varphi : P_1 \longrightarrow P_2$ de un orden $\langle P_1, \leq_1 \rangle$ en $\langle P_2, \leq_2 \rangle$ se dice *isótona* (o *creciente*) si se verifica:

$$x \leq_1 y \Rightarrow \varphi(x) \leq_2 \varphi(y).$$

Una función biyectiva $\varphi : P_1 \longrightarrow P_2$ de un orden $\langle P_1, \leq_1 \rangle$ en $\langle P_2, \leq_2 \rangle$ es un *isomorfismo de orden* si se verifica:

$$x \leq_1 y \text{ si y sólo si } \varphi(x) \leq_2 \varphi(y).$$

Decimos también que los órdenes P_1 y P_2 son *isomorfos*. Obsérvese que por tratarse de una biyección (inyectiva), la definición implica que

$$x <_1 y \text{ si y sólo si } \varphi(x) <_2 \varphi(y).$$

También es inmediato de la definición que si φ es un isomorfismo, $\varphi^{-1} : P_2 \longrightarrow P_1$ también lo es.

Es interesante observar que una biyección isótona no tiene por qué ser un isomorfismo de orden, como lo demuestra la función indicada en la Figura siguiente.

Figura 2. Una biyección isótona.

Ejemplo

El conjunto P de los enteros positivos pares con el orden heredado es isomorfo con \mathbb{N} . Basta definir

$$\begin{aligned}\varphi : \mathbb{N} &\longrightarrow P \\ n &\longmapsto 2n.\end{aligned}$$

No es tan directo demostrar que no existe un isomorfismo entre \mathbb{N} y \mathbb{Z} . Para verlo, supongamos que sí existe. Entonces consideramos $\varphi(0)$ y $\varphi(0) - 1 \in \mathbb{Z}$. Como φ es biyectiva (sobreyectiva), debe existir un entero positivo n tan que $\varphi(n) = \varphi(0) - 1$. Entonces $\varphi(n) < \varphi(0)$, luego por la definición de isomorfismo $n < 0$, lo que es una contradicción, por lo tanto no puede existir tal isomorfismo.

Este ejemplo ilustra el significado de que dos órdenes sean isomorfos: ambos deben tener las mismas propiedades de orden. En nuestro ejemplo, \mathbb{N} tiene un menor elemento y \mathbb{Z} no lo tiene, luego no pueden ser isomorfos. Por supuesto esta es una afirmación extremadamente vaga ya que no hemos dicho qué es una “propiedad” de orden. El siguiente teorema nos da una idea de lo que queremos decir y resulta muy útil para demostrar que dos órdenes NO son isomorfos.

Teorema 1. *Un isomorfismo de orden preserva mínimo, máximo, elementos minimales y maximales. Más precisamente, si φ es un isomorfismo y a es mínimo, máximo, minimal o maximal, entonces también lo es $\varphi(a)$.*

Más aún, φ preserva los cubrimientos, i.e. $a \prec b$ si y sólo si $\varphi(a) \prec \varphi(b)$.

Un ejemplo importante de ordenes isomorfos es el siguiente. Dado un conjunto X , consideremos el conjunto ordenado ${}^X\mathbf{2}$ de todas las funciones de X en $\mathbf{2} = \{0, 1\}$, que está ordenado por $0 < 1$.

Teorema 2. *Sea X un conjunto. Entonces $\langle \mathcal{P}(X), \subseteq \rangle$ es isomorfo con $\langle {}^X\mathbf{2}, \leq \rangle$.*

Demostración. Dado $A \in \mathcal{P}(X)$ definimos su *función característica* como sigue:

$$\begin{aligned}c_A : X &\longrightarrow \mathbf{2}, \\ c_A(x) &= \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases}\end{aligned}$$

Entonces

$$\begin{aligned}\varphi : \mathcal{P}(X) &\longrightarrow {}^X\mathbf{2} \\ A &\longmapsto c_A\end{aligned}$$

es un isomorfismo.

Para ver que φ es una biyección basta verificar que

$$A = B \quad \text{si y sólo si} \quad c_A = c_B,$$

es decir $c_A(x) = c_B(x)$ para todo $x \in X$.

Si $A \subseteq B$ y $c_A(x) = 1$, entonces $x \in A$, luego $x \in B$, y entonces $c_B(x) = 1$, por lo tanto $c_A(x) \leq c_B(x)$. Es claro que si $c_A(x) = 0$ entonces también $c_A(x) \leq c_B(x)$, luego para todo $x \in X$, $c_A(x) \leq c_B(x)$, o sea, por definición, $c_A \leq c_B$.

A la inversa, si $c_A \leq c_B$ y $x \in A$, $c_A(x) = 1$, luego $c_B(x) = 1$, o sea $x \in B$, vale decir $A \subseteq B$. Esto completa la demostración de que

$$A \subseteq B \quad \text{si y sólo si} \quad c_A \leq c_B,$$

y por lo tanto φ es un isomorfismo. \square

Teorema 3. *Todo orden es isomorfo con un orden de conjuntos.*

Demostración. Sea $\langle P, \leq \rangle$ un orden. Para cada $a \in P$, definimos $\mathcal{I}(a) = \{x : x \leq a\}$. Entonces si $Q = \{\mathcal{I}(a) : a \in P\}$, $\langle Q, \subseteq \rangle$ es un suborden de $\mathcal{P}(P)$ isomorfo con P . En efecto, definimos

$$\begin{aligned}\mathcal{I} : P &\longrightarrow Q \\ a &\longmapsto \mathcal{I}(a)\end{aligned}$$

Entonces, si $a \leq b$, y $x \in \mathcal{I}(a)$, $x \leq b$ y por lo tanto $\mathcal{I}(a) \subseteq \mathcal{I}(b)$.

Recíprocamente, si $\mathcal{I}(a) \subseteq \mathcal{I}(b)$, como $a \in \mathcal{I}(a)$, $a \in \mathcal{I}(b)$ y por lo tanto $a \leq b$.

Por otra parte, debido a la antisimetría, \mathcal{I} es inyectiva. La sobreyectividad es inmediata de la definición de Q . \square

1.4 Buenos Ordenes

Decimos que $\langle P, \leq \rangle$ es un *buen orden* (o que P está *bien ordenado*) si todo subconjunto no vacío de P contiene un menor elemento.

El ejemplo clásico de buen orden es el conjunto \mathbb{N} de los enteros positivos. Por su parte, \mathbb{Z} no está bien ordenado así como tampoco el intervalo $[0, 1]$ de los números reales con el orden heredado. En el primer caso el subconjunto \mathbb{Z} mismo no tiene menor elemento, en el segundo, el intervalo semiabierto (y obviamente no vacío) $(\frac{1}{2}, 1]$ no contiene su menor elemento.

Es fácil ver que un conjunto bien ordenado tiene que ser un orden total.

El siguiente teorema se puede demostrar en la teoría de conjuntos y es equivalente al axioma de elección.

Teorema 4. (de Zermelo)

Todo conjunto puede bien ordenarse.

El siguiente teorema es también equivalente al axioma de elección y juega un papel muy importante para resolver problemas más sofisticados en teoría de ordenes infinitos.

Teorema 5. (Lema de Zorn)

Si P es un orden tal que toda cadena tiene una cota superior, entonces P tiene un elemento maximal.

En todas las ramas de la matemática hay importantes aplicaciones del lema de Zorn. Por ejemplo:

1. Todo espacio vectorial tiene una base.
2. La unión enumerable de conjuntos enumerables es enumerable.
3. Existe un conjunto de números reales que no es Lebesgue-medible.
4. El producto de espacios compactos es compacto.
5. Todo anillo con unidad tiene un ideal maximal.
6. Todo orden parcial puede extenderse a un orden total.
7. El teorema de Hahn-Banach.
8. El teorema de completud para la lógica de primer orden.
9. Toda álgebra de Boole es isomorfa a un campo de conjuntos.

1.5 Ejercicios

1. ¿Cuántos ordenes parciales existen sobre $\{a, b\}$? ¿Sobre $\{a, b, c\}$? ¿Sobre $\{a, b, c, d\}$? Haga los diagramas correspondientes.
2. Diga cuáles de los órdenes del ejercicio anterior son isomorfos.
3. Dé los detalles de la definición del orden lexicográfico de los órdenes $\langle A_1, \leq_1 \rangle, \dots, \langle A_n, \leq_n \rangle$.
4. Demuestre que si P_1 y P_2 son órdenes con al menos dos elementos cada uno, entonces $P_1 \times P_2$ no es un orden total.
5. Demuestre que si P_1 y P_2 son ordenes totales, $P_1 \otimes P_2$ también lo es.
6. Demuestre que un conjunto bien ordenado es un orden total.
7. Use el buen orden de \mathbb{N} para demostrar el principio de indución. (De hecho ambas propiedades son equivalentes).

2 Retículos

Un elemento b es una *cota superior* de $A \subseteq P$ si para todo $a \in A$, $a \leq b$. Similarmente, c es una *cota inferior* de A si para todo $a \in A$, $c \leq a$.

Decimos que $\langle P, \leq \rangle$ es un *orden reticulado* o más simplemente un *retículo* si dados dos elementos cualesquiera a y b de P , siempre existen la menor de las cotas superiores de $\{a, b\}$, llamada el *supremo de a y b* , denotado $a \vee b$ y también la mayor de las cotas inferiores de $\{a, b\}$, llamada el *ínfimo de a y b* , denotado $a \wedge b$. De los órdenes que aparecen en la Figura 1, todos excepto (e) son retículos.

Teorema 6. *Sea $\langle P, \leq \rangle$ un orden reticulado. Entonces se verifican las siguientes identidades:*

R1 (Idempotencia)

$$x \vee x = x$$

$$x \wedge x = x$$

R2 (Conmutatividad)

$$\begin{aligned}x \vee y &= y \vee x \\x \wedge y &= y \wedge x\end{aligned}$$

R3 (Asociatividad)

$$\begin{aligned}x \vee (y \vee z) &= (x \vee y) \vee z \\x \wedge (y \wedge z) &= (x \wedge y) \wedge z\end{aligned}$$

R4 (Absorción)

$$\begin{aligned}x \vee (x \wedge y) &= x \\x \wedge (y \vee z) &= x\end{aligned}$$

Teorema 7.

$$x \leq y \quad \text{si y sólo si} \quad x \vee y = y \quad \text{si y sólo si} \quad x \wedge y = x.$$

Se puede dar una definición algo más abstracta de retículo que tiene la ventaja de que nos permite utilizar las herramientas teóricas del Álgebra Universal. En este contexto, un retículo es un álgebra $\langle L, \vee, \wedge \rangle$, donde L es un conjunto no vacío y \vee, \wedge son operaciones binarias sobre L que verifican las identidades R1–R4 del teorema anterior.

Podemos entonces entender los retículos de dos maneras: como órdenes que tienen supremos e ínfimos y como álgebras con dos operaciones que verifican ciertas propiedades. Estas perspectivas son complementarias.

La transición de una a la otra es muy intuitiva. Dado un orden reticulado $\langle P, \leq \rangle$, definimos el retículo $\langle P, \vee, \wedge \rangle$ de la manera obvia: $a \vee b$ y $a \wedge b$ son respectivamente el supremo y el ínfimo de $\{a, b\}$.

Por su parte, si $\langle L, \vee, \wedge \rangle$ es un retículo, podemos recuperar el orden sobre L mediante

$$x \leq y \quad \text{si y sólo si} \quad x \vee y = y \quad \text{si y sólo si} \quad x \wedge y = x.$$

EJEMPLOS

1. Todo orden total es un retículo con operaciones:

$$a \vee b = \text{máximo}\{a, b\}$$

$$a \wedge b = \text{mínimo}\{a, b\}$$

2. $\langle \mathbb{N}, | \rangle$ y el conjunto de todos los divisores de un cierto entero positivo n ordenados por divisibilidad son retículos. Aquí

$$a \vee b = \text{m.c.m.}\{a, b\}$$

$$a \wedge b = \text{M.C.D.}\{a, b\}$$

3. El conjunto $\{1, 2, \dots, 10\}$ ordenado por divisibilidad no es un retículo. En efecto, por ejemplo, no existe el supremo de 2 y 7. Obsérvese que sí existen los ínfimos de cualquier par de elementos.

4. Para cualquier conjunto X , el orden $\langle \mathcal{P}(X), \subseteq \rangle$ es un retículo con operaciones

$$a \vee b = a \cup b$$

$$a \wedge b = a \cap b$$

Este se llama un retículo de conjuntos o un *anillo de conjuntos*.

Un *subretículo* del retículo L es un subconjunto no vacío K de L que es cerrado bajo las operaciones \vee y \wedge de tal manera que $\langle K, \vee, \wedge \rangle$ es a su vez un retículo. Debe notarse que K debe estar dotado de la restricción de las operaciones de L a K . Ver ejemplo de la Figura 3 (a), en donde los puntos oscuros no forman un subretículo porque los supremos no coinciden.

Una función $\varphi : L_1 \longrightarrow L_2$ es un *homomorfismo* del retículo L_1 en L_2 si preserva las operaciones, es decir, si para todo $a, b \in L_1$ se verifica:

$$\varphi(a \vee b) = \varphi(a) \vee \varphi(b)$$

$$\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b)$$

Nótese que las operaciones \vee y \wedge que aparecen en el lado izquierdo son las de L_1 y las que aparecen en el lado derecho son las de L_2 . Dos retículos son *isomorfos* si existe un homomorfismo biyectivo entre ellos.

Cualquier función que preserve una de las dos operaciones es isótona, por ejemplo, si φ preserve ínfimos y $x \leq y$, se tiene que $x \wedge y = x$, luego

$$\varphi(x) \wedge \varphi(y) = \varphi(x \wedge y) = \varphi(x),$$

y por lo tanto $\varphi(x) \leq \varphi(y)$, luego φ es isótona.

Figura 3. Algunos ejemplos ilustrativos.

Debe observarse que hay una diferencia entre homomorfismos y funciones isótonas como lo ilustran los ejemplos de la Figura 3. En (b) no se preserva ninguna operación. En (c) se preservan ínfimos pero no supremos. Invertiendo el diagrama, se preservan sólo supremos. Por último (d) es una biyección isótona que no preserva ni ínfimos ni supremos.

Esta situación algo molesta no se presenta en el caso de isomorfismos de orden.

Teorema 8. *Dos retículos son isomorfos si y sólo si son isomorfos como órdenes.*

Demostración. Sea φ un isomorfismo del retículo $\langle L, \vee, \wedge \rangle$ en otro retículo. Como φ es una biyección isótona, falta verificar que su inversa φ^{-1} también lo es.

Supongamos que $\varphi(x) \leq \varphi(y)$. Entonces $\varphi(x) = \varphi(x) \wedge \varphi(y) = \varphi(x \wedge y)$ y como φ es inyectiva, obtenemos $x \leq y$.

Recíprocamente, sea φ un isomorfismo de órdenes. Como φ es isótona, $\varphi(x \wedge y)$ es una cota inferior de $\varphi(x)$ y de $\varphi(y)$. Supongamos que b es otra cota inferior. Como φ es sobreyectiva, existe $a \in L$ tal que $\varphi(a) = b$, luego

$$\varphi(a) \leq \varphi(x) \quad \text{y} \quad \varphi(a) \leq \varphi(y),$$

y como φ^{-1} es isotona, tenemos

$$a \leq x \quad \text{y} \quad a \leq y,$$

o sea, $a \leq x \wedge y$ y por lo tanto $b = \varphi(a) \leq \varphi(x \wedge y)$, por lo tanto $\varphi(x \wedge y)$ es la mayor de las cotas inferiores de $\varphi(x)$ y de $\varphi(y)$, o sea, $\varphi(x \wedge y) = \varphi(x) \wedge \varphi(y)$. \square

Ejemplo

Consideremos los retículos $\langle \mathbb{N}^{lc}, m.c.m., M.C.D. \rangle$, donde \mathbb{N}^{lc} es el conjunto de los enteros positivos libres de cuadrados, y $\langle \mathcal{P}_0(A), \cup, \cap \rangle$, donde A es un conjunto infinito enumerable. Estos retículos son isomorfos.

Es fácil ver que si A y B son dos conjuntos infinitos enumerables, $\mathcal{P}_0(A)$ y $\mathcal{P}_0(B)$ (y también $\mathcal{P}(A)$ y $\mathcal{P}(B)$) son isomorfos, luego podemos pensar que A es el conjunto de los números primos. Definimos

$$\begin{aligned} \varphi : \mathbb{N}^{lc} &\longrightarrow \mathcal{P}_0(A) \\ n &\longmapsto \{p \in A : p|n\} \end{aligned}$$

La función es un isomorfismo de órdenes, luego también es un isomorfismo de los retículos.

Dados retículos L_1, \dots, L_n , su *producto directo* es el retículo cuyo universo es el producto cartesiano $L_1 \times \dots \times L_n$ y cuyas operaciones están definidas por coordenadas, es decir

$$\begin{aligned} (a_1, \dots, a_n) \vee (b_1, \dots, b_n) &= (a_1 \vee b_1, \dots, a_n \vee b_n) \\ (a_1, \dots, a_n) \wedge (b_1, \dots, b_n) &= (a_1 \wedge b_1, \dots, a_n \wedge b_n) \end{aligned}$$

La definición anterior puede extenderse de una manera más o menos obvia al producto directo de una familia infinita de retículos.

Teorema 9. *La clase \mathcal{R} de todos los retículos es cerrada bajo subretículos, productos directos (incluso infinitos) e imágenes homomorfas.*

2.1 Retículos Modulares y Distributivos

Un retículo se dice *distributivo* si satisface una (y como veremos, ambas) de las identidades siguientes:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad (1)$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \quad (2)$$

Todos los retículos de la subsección anterior son distributivos.

Los retículos de la Figura 4 no son distributivos. Como veremos más adelante, estos son paradigmáticos.

Figura 4. Retículos no distributivos

Teorema 10. *En un retículo se satisface la identidad (1) si y sólo si se satisface la identidad (2).*

Demostración. Supongamos que (1) es válida.

$$\begin{aligned}
 x \vee (y \wedge z) &= (x \vee (x \wedge z)) \vee (y \wedge z) && R4 \\
 &= x \vee ((x \wedge z) \vee (y \wedge z)) && R3 \\
 &= x \vee ((z \wedge x) \vee (z \wedge y)) && R2 \\
 &= x \vee (z \wedge (x \vee y)) && (1) \\
 &= x \vee ((x \vee y) \wedge z) && R2 \\
 &= (x \wedge (x \vee y)) \vee ((x \vee y) \wedge z) && R4 \\
 &= ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) && R2 \\
 &= (x \vee y) \wedge (x \vee z) && (1)
 \end{aligned}$$

luego (2) también es válida. La demostración en el otro sentido es similar. \square

Debe observarse también que en todo retículo se cumple

$$\begin{aligned}x \wedge (y \vee z) &\geq (x \wedge y) \vee (x \wedge z) \\x \vee (y \wedge z) &\leq (x \vee y) \wedge (x \vee z)\end{aligned}$$

luego sólo la “mitad” de las identidades (1) y (2) son interesantes.

Un retículo se dice *modular* si satisface:

$$\text{Si } x \leq y, \text{ entonces } x \vee (y \wedge z) = y \wedge (x \vee z).$$

Observamos en primer lugar que en todo retículo, si $x \leq y$, $x \vee (y \wedge z) \leq y \wedge (x \vee z)$.

Teorema 11. *Todo retículo distributivo es modular.*

Los teoremas siguientes nos dan una sorprendente caracterización de la modularidad y de la distributividad.

Teorema 12. (Dedekind)

L es modular si y sólo si no contiene un subretículo isomorfo con N_5 (Figura 4).

Demostración. Es claro que si N_5 es un subretículo de L , éste no es modular.

Supongamos ahora que L no es modular. Por la observación después de la definición de modularidad, esto significa que existen elementos a , b y c tales que $a < b$ pero $a \vee (b \wedge c) > b \wedge (a \vee c)$.

Entonces el retículo de la Figura 5 es un subretículo de L .

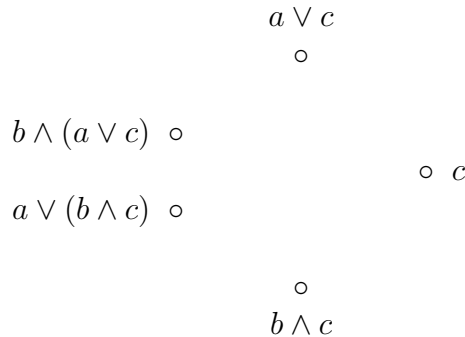


Figura 5.

Debemos entonces verificar que los ínfimos y supremos que aparecen en la Figura 5 son correctos. Lo que es inmediato es

$$b \wedge c < a \vee (b \wedge c) < b \wedge (a \vee c) < a \vee c,$$

o sea, el orden es correcto. Verificaremos algunos y los otros se dejarán como ejercicio.

$$[b \wedge (a \vee c)] \wedge c = b \wedge [(a \vee c) \wedge c] = b \wedge c,$$

por R3, R2 y R4. Similarmente

$$[a \vee (b \wedge c)] \vee c = a \vee [(b \wedge c) \vee c] = a \vee c.$$

□

Teorema 13. (Birkhoff)

L es distributivo si y sólo si no contiene un subretículo isomorfo con N_5 o con M_5 (Figura 4).

Demostración. Si L contiene un subretículo isomorfo con N_5 o con M_5 , es claro que no puede ser distributivo.

Recíprocamente, supongamos que L no es distributivo y que no contiene a N_5 como subretículo. Por el teorema anterior podemos suponer que L es modular.

Deberá existir elementos a , b y c tales que $(a \wedge b) \vee (a \wedge c) < a \wedge (b \vee c)$. Construiremos con ellos un retículo isomorfo con M_5 . Sean

$$\begin{aligned} d &= (a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \\ e &= (a \vee b) \wedge (b \vee c) \wedge (c \vee a) \\ a_1 &= (a \wedge e) \vee d \\ b_1 &= (b \wedge e) \vee d \\ c_1 &= (c \wedge e) \vee d \end{aligned}$$

Facilmente vemos que $d \leq a_1, b_1, c_1 \leq e$.

Debemos verificar que los ínfimos y supremos son los indicados en la Figura 6.

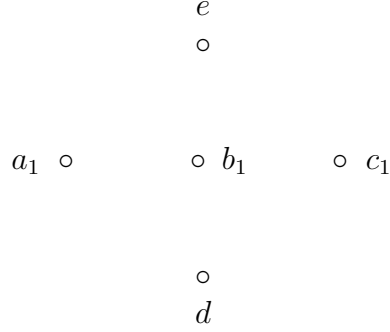


Figura 6.

Es fácil ver que $d \leq a_1, b_1, c_1 \leq e$.

Ademas por R4,

$$a \wedge e = a \wedge (b \vee c) \quad .$$

Aplicando la ley modular *Mod.* a los términos subrayados:

$$\begin{aligned}
a \wedge d &= \underline{a} \wedge ((\underline{a \wedge b}) \vee (a \wedge c) \vee (b \wedge c)) && \text{Mod. :} \\
&= (a \wedge \underline{b}) \vee (b \wedge c) \vee (a \wedge (b \wedge c)) && \text{R4 :} \\
&= (a \wedge b) \vee (b \wedge c)
\end{aligned}$$

de esta identidad, de la hipótesis y de (*) se sigue que $d < e$.

Verifiquemos por último una de las operaciones.

$$\begin{aligned}
a_1 \wedge b_1 &= ((a \wedge e) \vee \underline{d}) \wedge ((\underline{b \wedge e}) \vee d) && \text{Mod. :} \\
&= [(a \wedge e) \wedge ((\underline{b \wedge e}) \vee d)] \vee d && \text{Mod. :} \\
&= [(a \wedge e) \wedge ((b \vee d) \wedge e)] \vee d && \text{R2 :} \\
&= [(a \wedge e) \wedge e \vee (b \vee d)] \vee d && \text{R4 :} \\
&= [(a \wedge e) \wedge (b \vee d)] \vee d && (*) : \\
&= [(a \wedge ((\underline{b \vee c}) \wedge (\underline{b \vee (a \wedge c)}))] \vee d && \text{Mod. :} \\
&= [(a \wedge (b \vee ((\underline{b \vee c}) \wedge (a \wedge c)))] \vee d && a \wedge c \leq b \vee c : \\
&= (\underline{a} \wedge (b \vee (\underline{a \wedge c}))) \vee d && \text{Mod. :} \\
&= (a \wedge c) \vee (b \wedge a) \vee d \\
&= d
\end{aligned}$$

□

2.2 Un Teorema de Representación

Un *ideal* de un retículo L es un subconjunto no vacío \mathcal{I} tal que:

I1 Si $x \leq y$ y $y \in \mathcal{I}$, entonces $x \in \mathcal{I}$.

I2 Si $x, y \in \mathcal{I}$, entonces $x \vee y \in \mathcal{I}$.

Estrechamente relacionada con la noción anterior decimos que un subconjunto no vacío \mathcal{F} de L es un *filtro* si

F1 Si $x \geq y$ y $y \in \mathcal{F}$, entonces $x \in \mathcal{F}$.

F2 Si $x, y \in \mathcal{F}$, entonces $x \wedge y \in \mathcal{F}$.

Un *ideal* se dice *primo* si

IP1 $\mathcal{I} \neq L$.

IP2 Si $x \wedge y \in \mathcal{I}$, entonces $x \in \mathcal{I}$ ó $y \in \mathcal{I}$.

También podemos definir filtro primo (o *ultrafiltro* como es más habitual) de la manera obvia.

Lema 1. Si $X \subseteq L$ es no vacío, entonces existe el menor ideal que contiene a X . Lo llamamos el ideal generado por X .

Demostración. Basta observar que la intersección de todos los ideales que contienen a X es también un ideal que contiene a X . \square

Lema 2. Si \mathcal{I} es un ideal de L y $a \in L$ entonces el ideal $\mathcal{I}(a)$ generado por $\mathcal{I} \cup \{a\}$ es

$$\mathcal{I}(a) = \{x : x \leq a \vee y \text{ para algún } y \in \mathcal{I}\}.$$

Demostración. Ejercicio \square

El siguiente es uno de los teoremas más importantes dentro de la teoría de retículos.

Teorema 14. del Ideal Primo Sean L un retículo distributivo, \mathcal{I} un ideal y \mathcal{F} un filtro de L tales que $\mathcal{I} \cap \mathcal{F} = \emptyset$. Entonces existe un ideal primo \mathcal{J} tal que $\mathcal{I} \subseteq \mathcal{J}$ y $\mathcal{J} \cap \mathcal{F} = \emptyset$.

Demostración. Esta es una aplicación del Lema de Zorn (5). Sea P el conjunto de todos los ideales de L que contienen a \mathcal{I} y que son disjuntos de \mathcal{F} . $\langle P, \subseteq \rangle$ es un conjunto ordenado. Es fácil verificar que si C es una cadena de elementos de P , entonces $\bigcup C \in P$ es una cota superior de la cadena.

Por el Lema de Zorn, P contiene un elemento maximal \mathcal{J} , el que por definición es un ideal de L que verifica $\mathcal{I} \subseteq \mathcal{J}$ y $\mathcal{J} \cap \mathcal{F} = \emptyset$. Debemos ver que \mathcal{J} es primo.

Como $\mathcal{F} \neq \emptyset$, $\mathcal{J} \neq L$.

Supongamos que existen elementos $a, b \in L$ tales que $a \wedge b \in \mathcal{J}$ pero $a \notin \mathcal{J}$ y $b \notin \mathcal{J}$. Sean $\mathcal{J}(a)$ y $\mathcal{J}(b)$ los ideales generados por $\mathcal{J} \cup \{a\}$ y $\mathcal{J} \cup \{b\}$, respectivamente.

Por la maximalidad de \mathcal{J} , $\mathcal{J}(a) \cap \mathcal{F} \neq \emptyset$ y $\mathcal{J}(b) \cap \mathcal{F} \neq \emptyset$.

Usando el Lema 2 tomamos elementos $c, d \in \mathcal{J}$ tales que $a \vee c, b \vee d \in \mathcal{F}$. Como éste es un filtro, $(a \vee c) \wedge (b \vee d) \in \mathcal{F}$. Pero entonces por distributividad, $(a \vee c) \wedge (b \vee d) = (a \wedge b) \vee (a \wedge d) \vee (c \wedge b) \vee (c \wedge d) \in \mathcal{J}$, lo que contradice el que \mathcal{F} y \mathcal{J} son disjuntos. \square

Teorema 15. *Todo retículo distributivo es isomorfo con un retículo de conjuntos.*

Demostración. Sea L un retículo distributivo. Para cada $x \in L$ definimos

$$\widehat{x} = \{\mathcal{I} : \mathcal{I} \text{ es ideal primo de } L \text{ y } x \notin \mathcal{I}\}.$$

\widehat{x} no es vacío por el Teorema del Ideal Primo.

Veremos que para todo $x, y \in L$,

$$\begin{aligned}\widehat{x} \cup \widehat{y} &= \widehat{x \vee y}, \\ \widehat{x} \cap \widehat{y} &= \widehat{x \wedge y}.\end{aligned}$$

En efecto, si \mathcal{I} es primo

$$\mathcal{I} \in \widehat{x \vee y} \text{ ssi } \mathcal{I} \in \widehat{x} \text{ ó } \mathcal{I} \in \widehat{y} \text{ ssi } x \notin \mathcal{I} \text{ ó } y \notin \mathcal{I} \text{ ssi } x \vee y \notin \mathcal{I} \text{ ssi } \mathcal{I} \in \widehat{x \vee y}.$$

y similarmente

$$\mathcal{I} \in \widehat{x \wedge y} \text{ ssi } \mathcal{I} \in \widehat{x} \text{ y } \mathcal{I} \in \widehat{y} \text{ ssi } x \notin \mathcal{I} \text{ y } y \notin \mathcal{I} \text{ ssi } x \wedge y \notin \mathcal{I} \text{ ssi } \mathcal{I} \in \widehat{x \wedge y}.$$

Por lo tanto $\widehat{L} = \{\widehat{x} : x \in L\}$ es un retículo de conjuntos. Sólo tenemos que verificar que la función

$$\begin{aligned}\varphi : L &\longrightarrow \widehat{L} \\ x &\longmapsto \widehat{x}\end{aligned}$$

es un isomorfismo. Supongamos que $x \leq y$ y que $\mathcal{I} \in \hat{x}$, o sea $x \notin \mathcal{I}$. Entonces, si $y \in \mathcal{I}$, por I1, $x \in \mathcal{I}$, lo que es una contradicción, luego $y \notin \mathcal{I}$, o sea, $\mathcal{I} \in \hat{y}$, con lo que probamos $\hat{x} \subseteq \hat{y}$.

Por otra parte, si $x \neq y$ consideramos el ideal $(y]$ de los elementos menores que y y el filtro $[x)$ de los elementos mayores que x . Como $(y] \cap [x) = \emptyset$, por el Teorema del Ideal Primo, existe un ideal \mathcal{I} tal que $x \notin \mathcal{I}$ y $y \in \mathcal{I}$. Equivalentemente, $\mathcal{I} \in \hat{x}$ y $\mathcal{I} \notin \hat{y}$.

Esto demuestra que φ es un isomorfismo. □

2.3 Ejercicios

1. Si G es un grupo, entonces $S(G)$ y $N(G)$, respectivamente, el conjunto de todos los subgrupos de G y el conjunto de todos los subgrupos normales de G ordenados por \subseteq son retículos. ¿Cómo se definen las operaciones? Verifique si en general ellos son distributivos o modulares.
2. Demuestre el teorema 9, es decir, que la clase \mathcal{R} de todos los retículos es cerrada bajo subretículos, productos directos e imágenes homomorfas.
3. Haga lo mismo para la clase \mathcal{D} de todos los retículos distributivos.
4. Demuestre los dos lemas de la última sección.

Referencias

- [1] Balbes, R. and Dwinger, P., *Distributive Lattices*, University of Missouri Press, 1974.
- [2] Birkhoff, G., *Lattice Theory*, A.M.S. Colloquium Publications, Vol. XXV, 1973.
- [3] Halmos, P., *Lectures on Boolean Algebras*, van Nostrand Company, 1963.
- [4] Hamilton, A. G., *Numbers, sets and axioms*, Cambridge University Press, 1982.